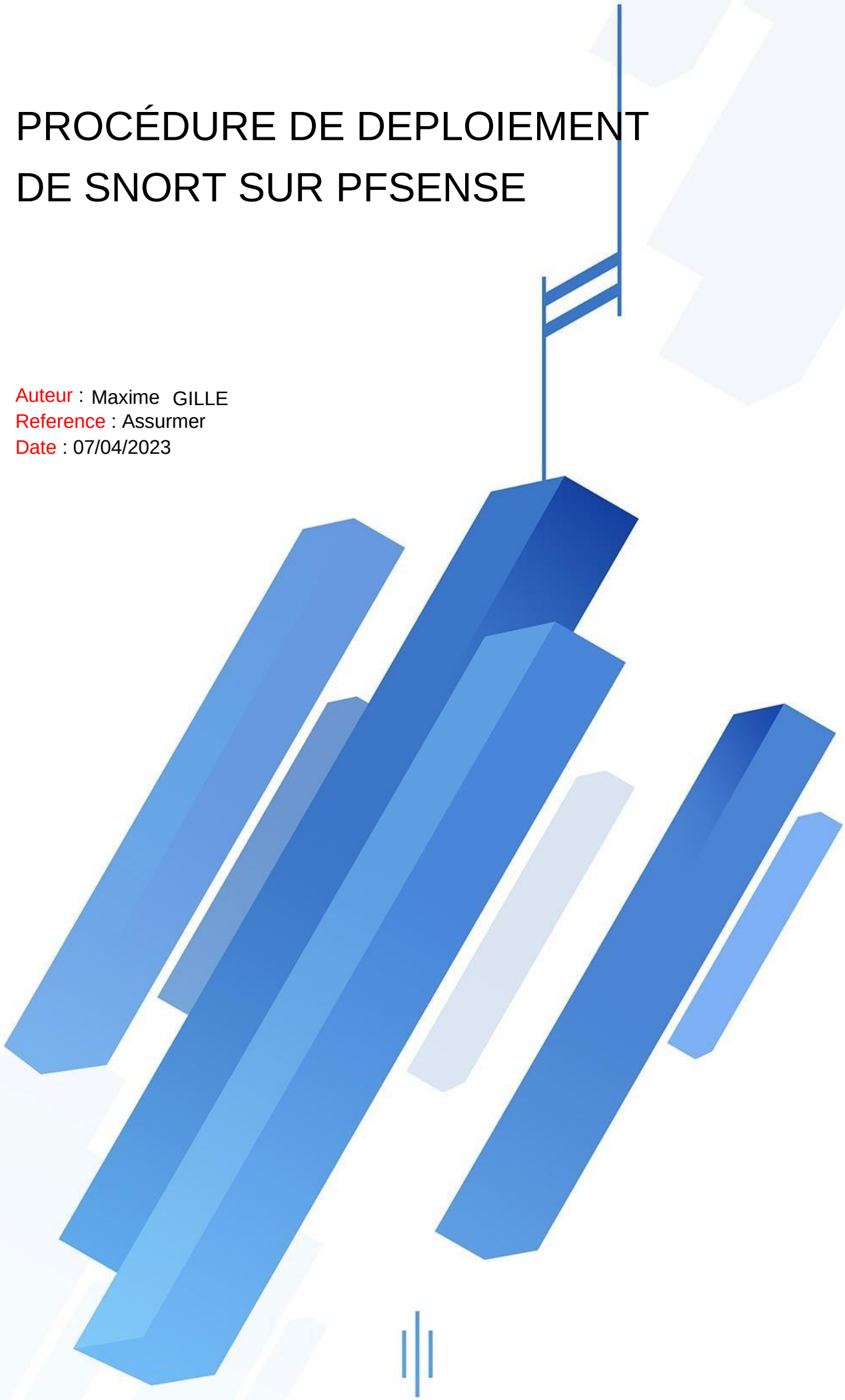
PROCÉDURE DE DEPLOIEMENT DE SNORT SUR PFSENSE

Auteur : Maxime GILLE
Reference : Assurmer
Date : 07/04/2023



DIFFUSION et VISAS

Diffusion				
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**	**Pour info**
Assumer	Service IT	Procédure	Réseau	

Visas			
Société/Entité	**Nom**	**Fonction**	

SUIVI DES VERSIONS

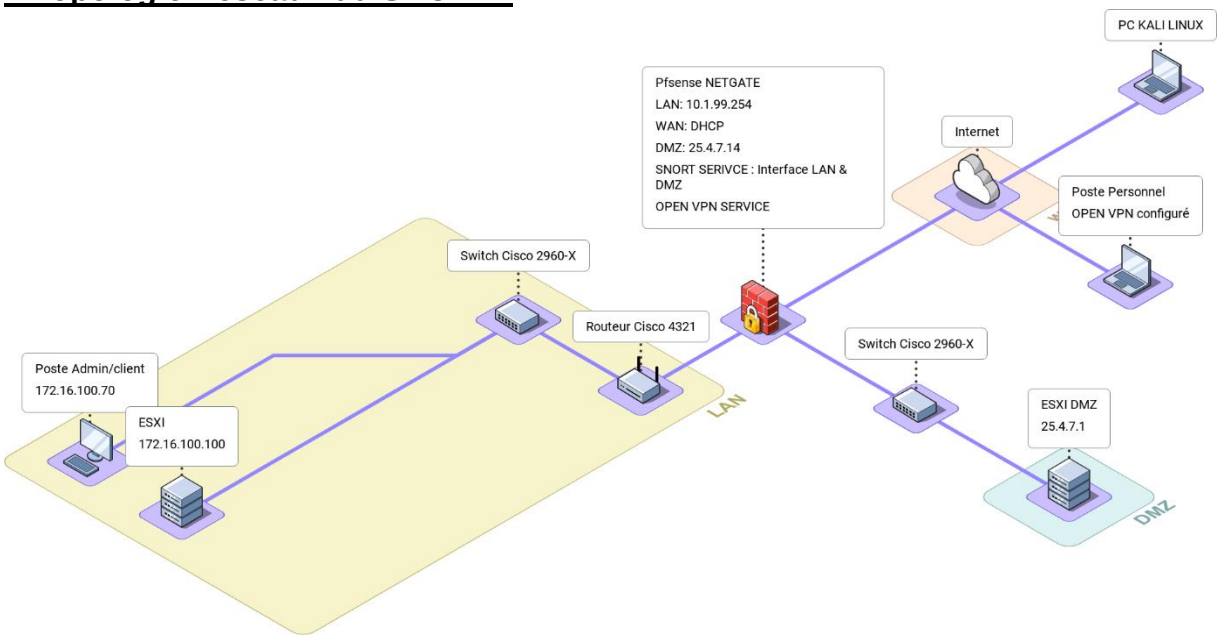
Version	Date	Auteur	Raison	Nombre de pages
V1.0	07/04/2023	Maxime GILLE	Procédure d'installation de SNORT sur PFSENSE	8

COORDONNEES

Contacts		
Nom	**E-mail**	**Téléphone**
Maxime GILLE	maxime.gille@edu.esiee-it.fr	06.43.09.98.54

Table des matières

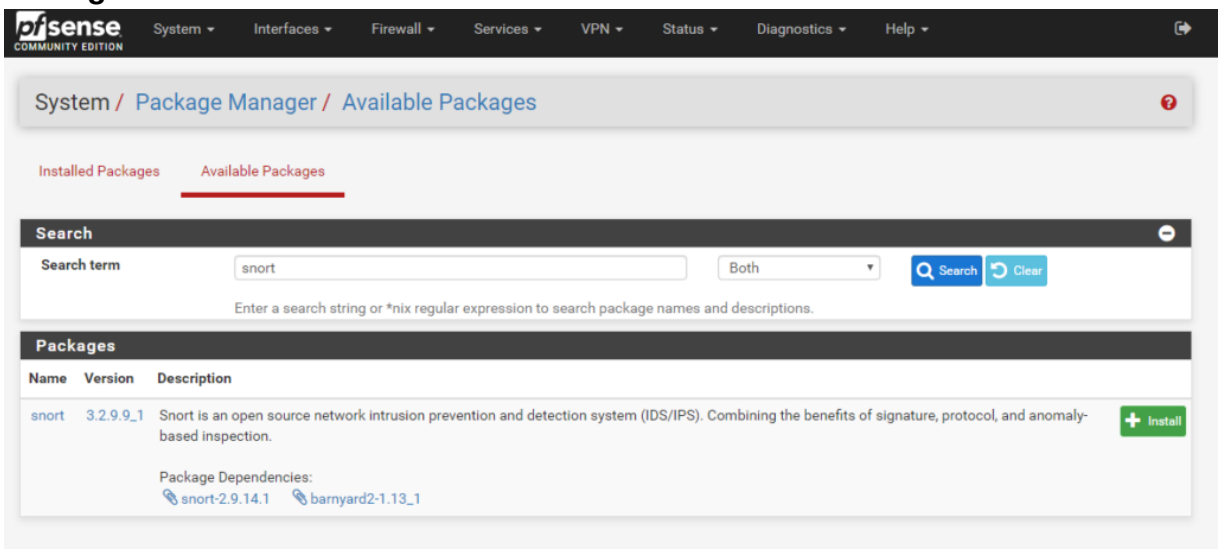
1.Topologie Réseaux du SNORT :



2.Configuration de la Solution SNORT :

Installation de SNORT :

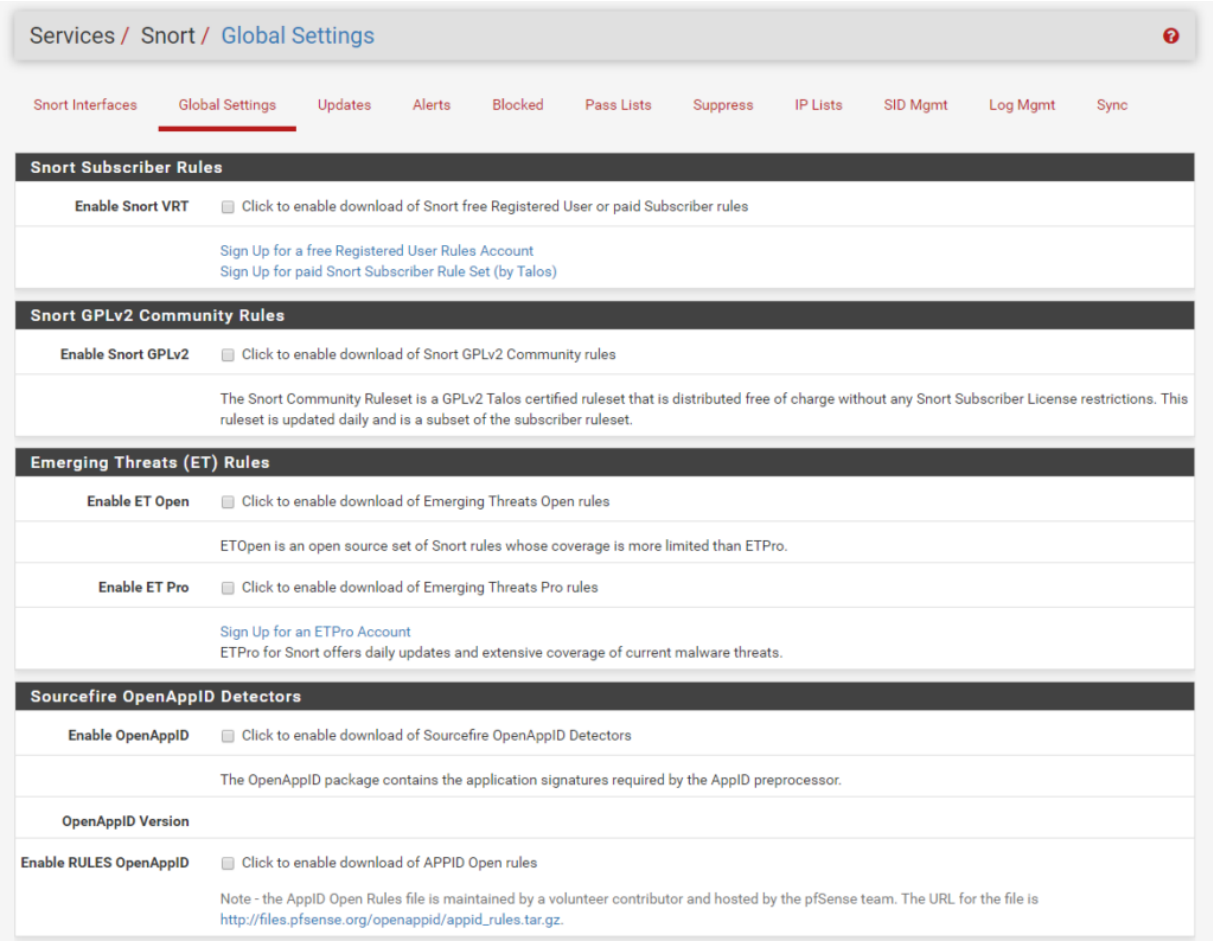
Une fois notre **PFSENSE** installé et configuré, nous nous rendons dans le **Packet Manager** :



On clique ensuite sur **Install** puis **Confirm** et l'installation se lance ! Rien de très compliqué donc.

Configuration de SNORT :

Une fois installé, Snort apparaîtra dans l'onglet **Services**. Une fois rendu dessus, nous allons dans un premier temps aller sur l'onglet **Global Settings** :

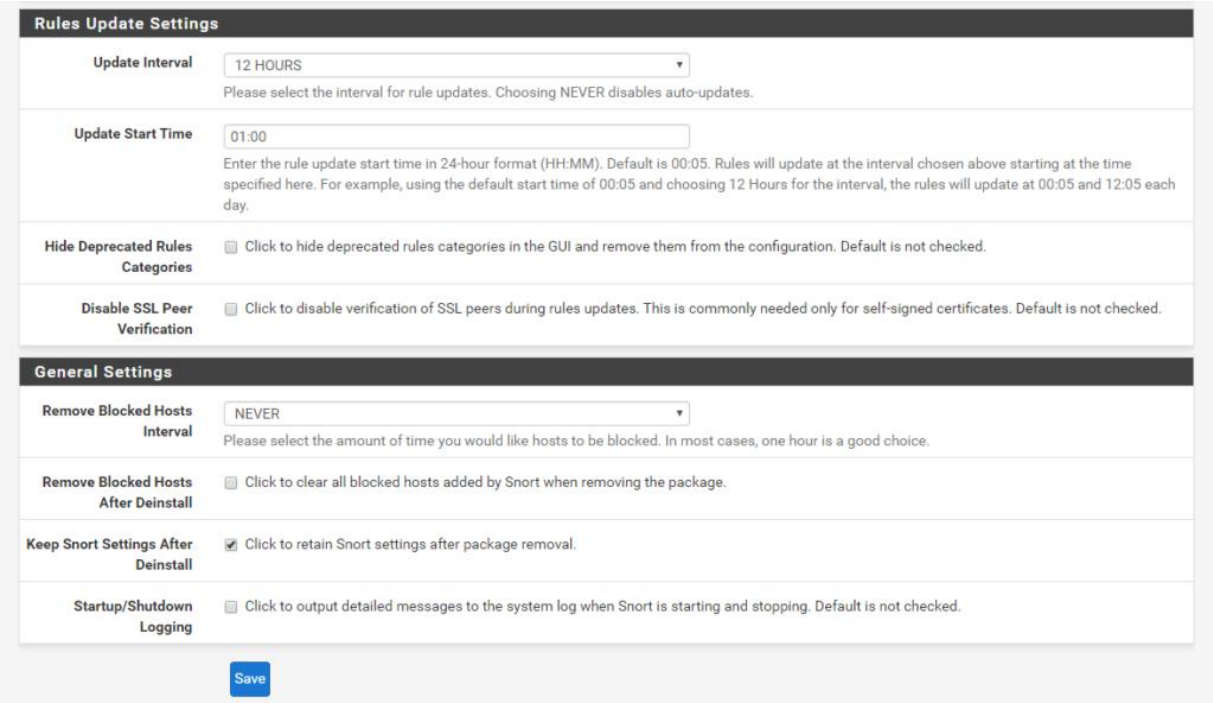


La première étape est donc d'activer le téléchargement de règles gratuites, en cochant la première case (**Enable Snort VRT**). Il faudra renseigner une clé et pour l'obtenir il vous faudra créer un compte sur le site officiel de Snort.

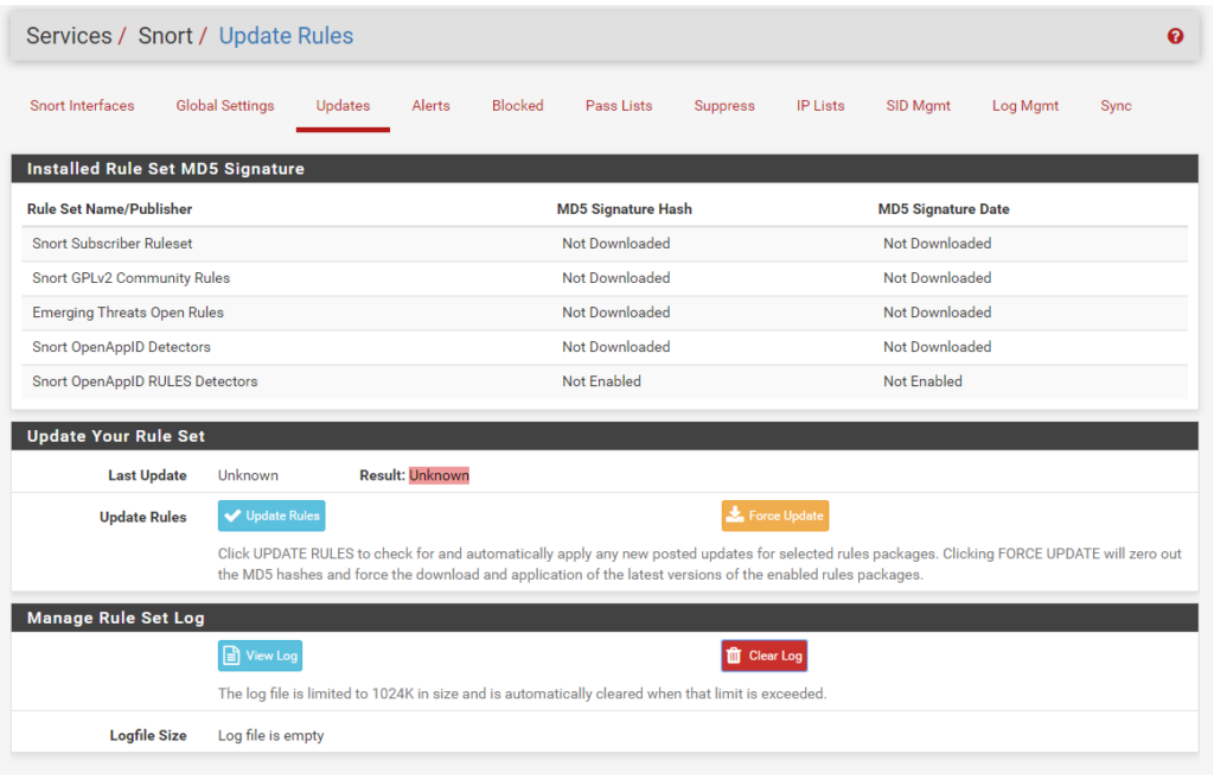
Et ensuite nous pouvons cocher les cases :

- **Enable Snort GPLv2**, pour les règles communautaires ;
- **Enable ET Open**, qui sont des règles proposées par la société ET ;
- **Enable OpenAppID**, éventuellement, qui est une autre société ;

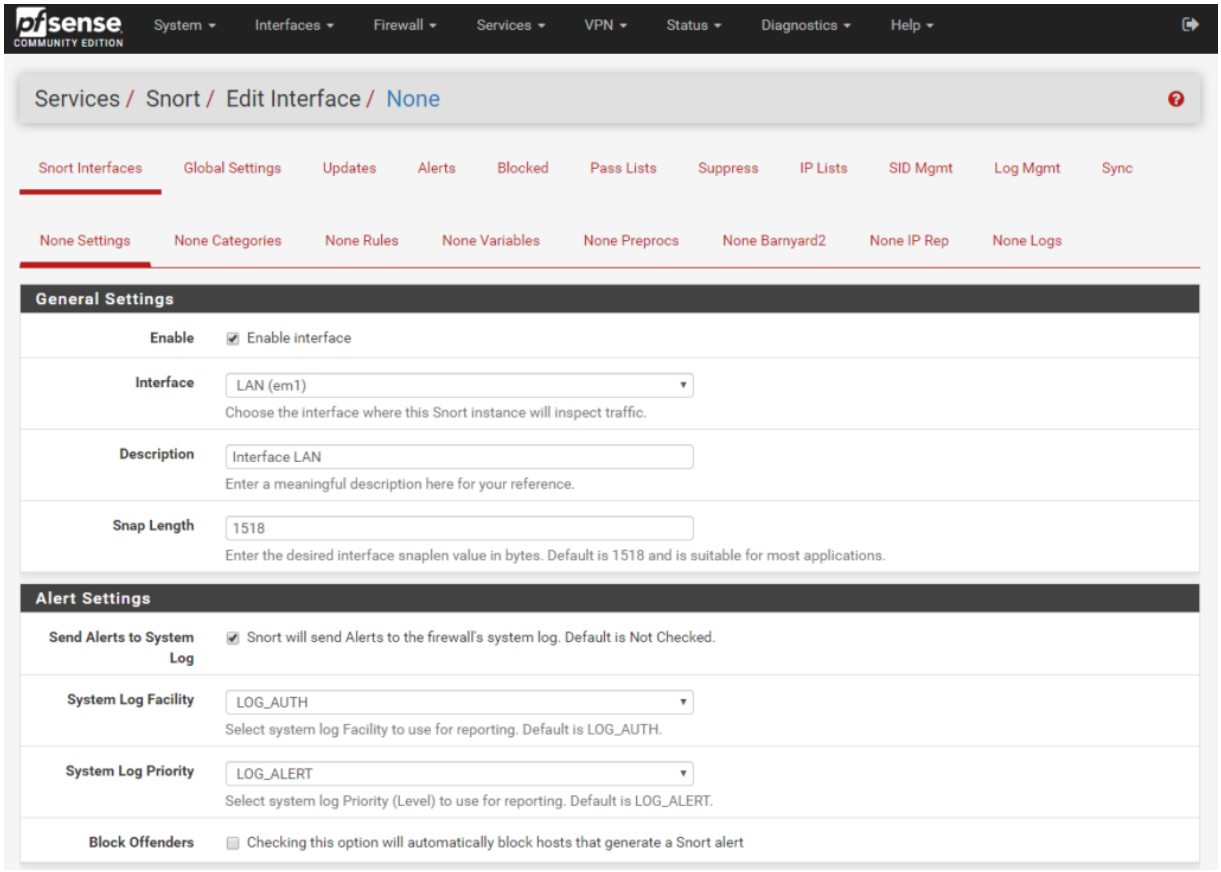
Et ensuite, pour les derniers paramètres il convient simplement de configurer l'update pour les différentes règles, c'est-à-dire le délai avant de vérifier les mises à jour pour les différentes règles ou pour de nouvelles :



Une fois cliqué sur **Save**, nous pouvons nous rendre sur l'onglet **Updates** et manuellement mettre à jour les différentes règles que nous avons cochées juste avant:

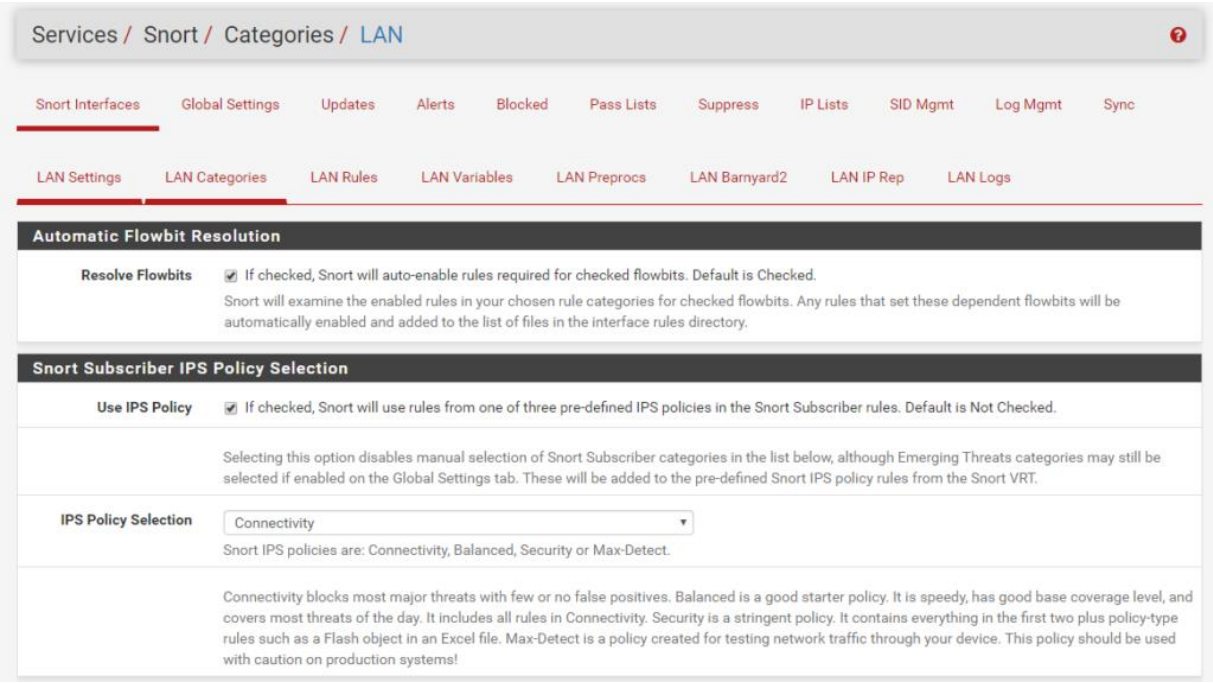


Une fois la mise à jour terminé, nous approchons de la fin ! Rendons-nous donc sur **Snort interfaces** pour choisir l'interface sur laquelle Snort va écouter et analyser le trafic :

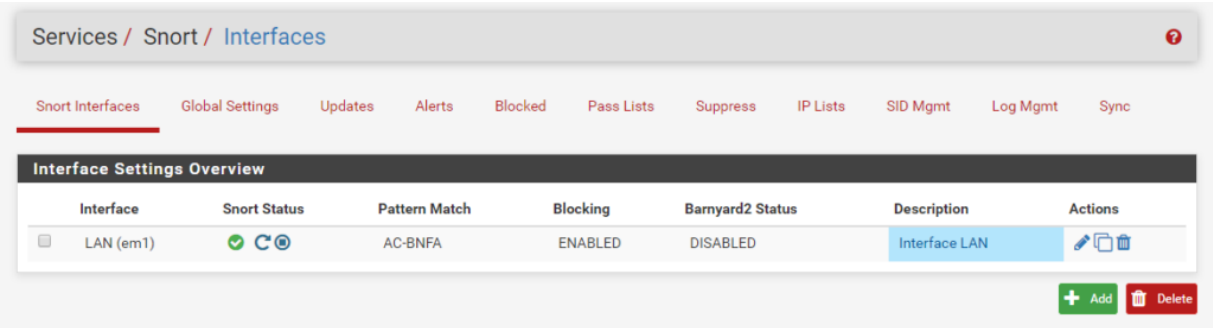


Pour Assurmer nous allons demander au **PFSENSE** d'analyser le trafic de l'interface **LAN & DMZ.**

L'avant dernière étape est d'activer toutes les règles précédemment téléchargées en nous rendant dans **LAN Categories**, sur **Snort Interfaces**, **LAN** en cochant l'option **Use IPS Policy** :



On valide, et on retourne à la liste des interfaces de Snort pour cliquer sur **Start** :



Voilà **SNORT** est configuré sur le **PFSENSE** d'Assurmer afin de prévenir d'éventuelle intrusion.